EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 16 — March 14, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Cyclic Groups

2 Cyclic Groups

- **Proposition:** Let G be a finite group. Assume multiplicative notation for the group operation. For $g \in G$, the set $\langle g \rangle = \{g, g^2, g^3, \ldots\}$ is a subgroup of G.
- $\langle g \rangle$ is called the *subgroup generated by* g. If the order of the subgroup is i, then i is called the *order of* g.
- Let G be a finite group and $g \in G$. The *order of* g is the smallest positive integer k with $g^k = 1$ where 1 is the identity of G.
- **Proposition:** Let G be a finite group of order m and let $g \in G$ have order k. Then $k \mid m$.
- **Definition:** A cyclic group is a finite group G such that there exists a $g \in G$ with $\langle g \rangle = G$. We say that g is a *generator of* G.
- **Proposition:** If G is a group of prime order p, then G is cyclic. Furthermore, all elements of G except the identity are generators of G.
- **Definition:** Groups G and H are isomorphic if there exists a bijection $\phi : G \to H$ such that

$$\phi(\alpha \star \beta) = \phi(\alpha) \otimes \phi(\beta)$$

  for all $\alpha, \beta \in G$. Here $\star$ is the binary operation in G and $\otimes$ is the binary operation in H.
- Example of group isomorphism
  - $\mathbb{Z}_2 = \{0, 1\}$ is a group under modulo 2 addition
  - $R = \{1, -1\}$ is a group under multiplication

$\mathbb{Z}_2$	R
$0 \oplus 0 = 0$	$1 \times 1 = 1$
$1 \oplus 0 = 1$	$-1 \times 1 = -1$
$0 \oplus 1 = 1$	$1 \times -1 = -1$
$1 \oplus 1 = 0$	$-1 \times -1 = 1$

- **Theorem:** Every cyclic group G of order n is isomorphic to $\mathbb{Z}_n$ with addition modulo n as the operation.
- **Corollary:** Every cyclic group is abelian.

2.1 Subgroups of Cyclic Groups

- **Theorem:** Every subgroup of a cyclic group is cyclic.
- Example: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has subgroups $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\{0, 1, 2, 3, 4, 5\}$
- Proof
  - If h is a generator of a cyclic group G of order n, then

$$G = \left\{h, h^2, h^3, \dots, h^n = 1\right\}$$

  - Every element in a subgroup S of G is of the form h^i where $1 \leq i \leq n$
  - Let h^m be the smallest power of h in S
  - Every element in S is a power of h^m

3 References and Additional Reading

- Section 8.3 from Katz/Lindell
- Section 7.3 of lecture notes of MIT's Principles of Digital Communication II, Spring 2005. `https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-451-principles-readings-and-lecture-notes/MIT6_451S05_FullLecNotes.pdf`
- Section 2.4 of *Topics in Algebra*, I. N. Herstein, 2nd edition
- Section 8.1.4 from Katz/Lindell